DATABASE ACCESS METHOD AND SYSTEM FOR USER ROLE DEFINED ACCESS

FIELD OF THE INVENTION

The invention relates to determination and granting of access to data and files by the file or database creator, owner or manager or by group or user access profiles.

BACKGROUND

Current database management applications and especially the access subsystems thereof support what could be called a "Single Organization Model". This means that all users of a system, even though they may work in various divisions of a company or various channels of a marketing organization, or even different entities leasing portions of the same database through a common vendor or service organization, are deemed to ultimately work for the same organization, and that organization is at the root of the organizational hierarchy.

Present access control mechanisms, built on the "Single Organization Model," are cumbersome when applied to multi-divisional or multi-channel organizations or to multi-tenant databases. This is because present access authorization systems are adapted to: (1) partition data to show users only those records that they or their position have been granted visibility to, and (2) show users all "global" data in a particular dataset. However, absent cumbersome "work arounds" present access authorization subsystems do not have the ability to partition data at the organizational or channel level. This makes it impossible, for instance, for companies using the "e-channel marketing" paradigm that do business in multiple countries in Europe to maintain separate price lists for each country and have only those price lists that are appropriate for a region or country be accessible. This cumbersome access control also makes it difficult for multiple small financial service organizations to outsource database and telephone support operations to a common vendor while preserving customer confidentiality.

SUMMARY

The invention is a database management system and a method of using the system. The system has an access control subsystem, and is characterized by a plurality of user entries representing users seeking access to data items, where each of the user entries has at least one organizational access attribute. The data stored in the underlying database has a plurality of data items. Each of the data items may be a data file, a data field within a data file, or a view of a data items. Selected ones of the data items have at least one organizational access attribute. This organization attribute is used by the access control subsystem. The access control subsystem receives a database query from a user requesting access to one or more of the data items. The access control subsystem reads the user's organizational access attributes, and reads the data item's organizational access attributes. The access control subsystem then presents data items to the user to which the user has access authorization.

In one embodiment of the invention, particularly useful in channel marketing and in multi-divisional enterprises, the database files have a plurality of fields, and the users have personal, positional, and organizational attributes, and are divisible into multiple membership sets based upon organizational attributes. The database views are visible to users based upon the personal, positional, and organizational attributes of the users.

The data files and fields may extend across organizations, or they may be disjoint, extending to only one organization. Likewise, the users may be in overlapping organizations, or in only one organization.

According to this embodiment of the invention, the views visible to a user are determined by the user's organizational and positional attributes, and the view files are determined by a user's organizational and/or positional attributes. In a still further embodiment, the view files are determined by a user's organizational attributes, and view fields are determined by a user's positional attributes.

In an alternative embodiment of the invention a plurality of organizations exclusively own individual data files in the database management system. An individual data file has a single owner. The access control subsystem is configured to authorize a customer of the owner

organization to have access to their own data items and to grant access to their own data items to an additional user, for example, a telephone service representative, while the customer accesses the data items. The customer can authorize the additional user to access and update the data item.

In this embodiment, the database system may be regarded as a partitionable database with a plurality of separate virtual databases. Each of the separate virtual databases may have a unique database owner, and a user can only access files in a virtual database to which the user has access authorization from the database owner.

The separate virtual databases may be disjoint, for example with common ownership or separate and unique owners. Access may depend upon authorization from the database owner to access either the database or a file within the database, and where the user requesting access is not the owner of the file, access may require authorization from the owner of the file. This situation typically occurs in a multi-tenant database having a plurality of tenants, where each tenant is the owner of a separate virtual database, and at least two of the tenants utilize a common call center service, as is the case with a large financial institution servicing the customer accounts of other financial institutions.

THE FIGURES

The method and system of the invention are illustrated in the FIGURES.

FIGURE 1 represents a simplified, high level view of the schema of a database of the "multi-organization support" method and system of the invention.

FIGURE 2 represents a simplified, high level view of the schema of a database of the "multi-tenancy support" method and system of the invention.

OVERVIEW

This invention relates to database access and more particularly to methods and systems for controlling database access through an access authorization subsystem of the database management system. The access authorization subsystem utilizes user and data attributes that have utility beyond database access or visibility; the access authorization subsystem filtering,

screening, and querying these attributes to determine access or visibility of a user to a data item. The ability to dynamically support database access based upon the instantaneous role of the user at the time of access, that is, in real time, requires a user role defined access authorization subsystem such as the "Multiple Organization Model," having a schema as shown at a very high level in FIGURE 1, or "Multi-Tenant Model," having a schema as shown at a very high level in FIGURE 2.

The concept of the "multiple organization model" or "multi-organizational" support is especially important to e-channel marketing. The driving force behind e-channel marketing is that multiple channel partners share a common database, including business objects and tools, with the main company. Each of the channel partners should only see data that is relevant to their own organization. This means that they would not see data for other channel partners or non-global data from the parent organization.

Similarly, the concept of the "Multi-Tenant Model" or "Multi-Tenant Support" is especially important to small financial service providers, retailers, and the like. This is because multi-tenant support enables these businesses to out source, for example, their credit card operations to a service agency or large financial services organization, with the telephone support staff member of the large financial services organization having gaining real time access to the individual account being serviced during the service call.

DETAILED DESCRIPTION

This invention relates to database access where a user's access rights to specific data items are defined dynamically, that is, in real time, based upon the user's status at the time of access request, and data and user attributes having independent utility and significance apart from access and visibility. Colloquially, the user has one set of access authorizations while wearing a red hat and another set of access authorizations while wearing a blue hat. The hats could represent roles as a telephone service representative for multiple credit card issuers sharing a multi-tenant, vendored, database, or roles as a marketing representative of a company in first and second regions.

The database access system and method of the invention utilizes a division of the data "owners" either (1) hierarchically, that is vertically, with horizontal divisions in branches, or (2) horizontally, that is, separate virtual databases. The database itself is divided into files, the files are divided into records within the files, and individual records are divided into fields. In either mode of division, the (schema and metadata data needed and would be sophisticated), and user access is based upon user's relationship to one or more owners in the hierarchy. (for example, owners could be independent lessees of database capacity or divisions in a multi-divisional enterprise).

The method and system of the invention builds upon partitionability of the individual database files in the database based upon an attribute of ownership and/or control. For example, in the multi-tenancy model, the database might be partitionable into separate and distinct individual virtual databases, as in the case of financial services organizations, for example competing financial services organizations, vendoring database capacity, database management services, and telephone support services for a service provider. By way of contrast, in the multi-organization support model, the database's parent organizational owner is hierarchically and organizationally divisible, for example into divisions, departments, and offices, where each branch point may be a hierarchical level and each branch may be a functional owner of a portion of the enterprise database.

In both embodiments user access is triggered by a "need to know" or "convenient to know." In the multi-tenancy embodiment, the access is typically triggered by an incoming call to a vendored call center, and the view is the customer's computer telephony integration (CTI)-identified account number. Similarly, in the multi-organization support embodiment, the access is triggered end user action, and the specific view is triggered by the end-user's logon, that is, which division or channel or reporting chain is used for this task.

Multi Organization Support

In a large organization where the same products and/or services are rendered through different employees and/or rendered to different customers, or where some goods, services, or customer sets are prohibited to some employees or organizations and permitted to others (for example, sale of encryption equipment or code to the PRC, or the sale with English only labeling/instructions

in Quebec), and the product set is too large and/or unwieldy to maintain separate databases, there is a definite productivity advantage to organizationally limiting access so that the marketing representative is not inundated with "useless" information. This is accomplished by assigning access authorization organizationally, including regionally. This way, when a sales or service rep or a channel partner enters a "MYLIST" command, he or she is only presented with a virtual database of the products and/or services that he or she can actually render. This is the "single database – multiple independent users" embodiment, also referred to as the "multi-organization support" method and system.

FIGURE 1 is a very high level view of the database schema of a "multi-organization support" model. The schema, 1, has, for purposes of illustration, five fields in each record. These fields are the Sales Rep, 11, the Division, 13, the Profit Center (within the Division, 13), 15, the customer 17, and the sales to that customer in the year 2000, 19. Sales Representative Patterson, 21, is in the Microelectronics Division 21A, 21B, and sells in two profit centers of the division, cards, and chips. Hennessey, 23 is in only one Division, the Server Division, 23A, and sells the goods of only one profit center, RISC 6000. Also in the Server Division, 25B, is Streetman, 25, who only sells the product of one profit center, the AS400 profit center. Sales Representative Sze, 27, is also in the Server Division, here 27A, and only sells the products of one profit center, the ENT 9000 profit center.

The multi-organization support utilizes new types of visibility attributes called "organization" and "organization team" visibility. In the multi-organization support method and system of the invention, the records that a user sees with "organization" and "organization team" visibility are restricted based upon the organization(s) that the user has been given visibility into, while the ones the end user sees with "position" and "position team" visibility are restricted based upon the user's current position. While there may be some overlap between "organization" attributes and "position" attributes, they may confer different rights. For example, "organization" attributes may only confer "read" authorization, while "position" attributes may confer "read," "write", and "delete" authorization. The "organization" and "organization team" visibility is used in a series of "My Organization's" views that show all of the data that the user's organization has been granted visibility to. In this way, multiple organizations can share the same database but

see a partitioned set of data that is pertinent to them. It is also to be understood, that there may be inheritance of access up and down and across a hierarchy.

One access attribute specifies the visibility attributes of the higher level organization, for example a division. This means that the number of distinct organizational partitions will be relatively small compared to the overall number of divisions in the hierarchy. Also, organizational partitions should be relatively high in the hierarchy. Therefore, most of the lower level entities in a large enterprise, for example a domestic marketing division of a large international enterprise may reference the US division as their visibility organization. This would enable all people who work for any of those lower level product or marketing organizations to see the same partition of data.

The relationship between divisions and positions is normally a 1-to-many relationship, although the system and method of our invention can support a many-to-many relationship. That is, a position belongs to exactly one division. If a user needs to have access to data in multiple organizations, then the user would be required to have positions in the appropriate organizations, or, in an alternative embodiment of our invention, to have personal or positional access to the data separate and apart from but in addition to his or her organizational access to the data. This could be done by having positions specifically for granting visibility to users outside of the organization.

Single organization ownership is added to an entity by adding a foreign key to the owning organization and configuring the business component appropriately. Organization teams are added to an entity by adding an intersection table between that entity and organization and a foreign key to the primary owning organization, and configuring the business component appropriately.

During login, while the system is collecting information about the positions a user is associated with, the system looks at the user's division or divisions and collects the set of organizations those divisions have visibility into. If a user has n positions, that is, n positional attributes, the user will have between 1 and n organizations for visibility.

The organization and organization team visibility's are used for "My Organization's" views to show the user all of the records for the entity where the user's "current" organization is either the owner, or on the organization team. The user's "current" organization will be the visibility organization assigned to the division of the user's current position. When a user changes current position, the current organization will be changed automatically.

Channel Partners may be administered by creating a division node or hierarchy as the visibility organization in the appropriate table. All sub-organizations for that channel partner should specify the root channel partner division node as the visibility organization. Similarly, the Pick Lists and association lists for entities that are "multi-org'd" will show the appropriate organization specific data.

Channel partners may either assign access authorization to their own users or request the database owner to assign access authorization.

Multi Tenancy Support

An alternative embodiment of our invention is the "multiple tenancy" model described with respect to CTI applications. This embodiment solves problems associated with the situation of a plurality of merchants and/or financial services organization vendoring out their telephone service and data processing operations to a common vendor. The common vendor stores the merchants' and institutions' customer accounts in an access controlled database while also providing customer telephone support service for the customer accounts. That is, the CTI (computer-telephony integration) automatically switches the agent to the correct slice (that is, customer files) of the database. Access to a customer account is authorized in real time during the individual telephone support session with the customer. During the individual customer support session, the telephone support representative has access to the individual merchant's or financial institution's business objects, queries, and views, as well as those of the database service provider.

FIGURE 2 shows a very high level view of the "multi-Tenant" database schema, 1. This schema shows three banks in the Bank column 31, CITI 43, MBNA, 45, and BankOne, 45. In the

customer column, 33, each bank is shown with only two customers, McCabe 43A and Smith 43B for CITI, 43, Van Ness 45A and Bird, 45B for MBNA, 45, and Stewart, 47A, and Lightfoot, 47B, for BankOne 47. Each customer has an account number, shown in column 35, and space for the last three transactions, shown in columns 37, 39, and 41. In operation, if VanNess were to call the Vendor's support center on the appropriate access number, and properly enter the account number shown for VanNess in column 35, line 45, VanNess's account would come up on the CTI operator's screen, and both VanNess and the CTI operator would have access to account information.

To be noted is that when a caller calls in to an outsourcing call center or multi-tenancy call center, the gets switched to the slice of the database for that tenant (for example, the slice of the database assigned to their financial service provider) not just the particular file for that particular caller or customer. This is important because in this way the customer can access information about Products, Price Lists, Service Requests and Sevices of their tenant that is being provided by the tenant, either directly or through outsourcing.

While the invention has been described with respect to certain preferred embodiments and exemplifications, it is not intended to limit the scope of the invention thereby, but solely by the claims appended hereto.